EDOK - Application for Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of: **The property to be searched is described as a Cloud Mobile Stratus C7, IMEI: 356225738710543, ("Device 3"). Device 3 is currently in the possession of the Drug Enforcement Administration, McAlester Resident Office (MRO), at 100 Airport Road, McAlester, Oklahoma, located within the Eastern District of Oklahoma.**	**Case No.** 24-MJ-315-JAR

APPLICATION FOR SEARCH WARRANT

I, Charles Sutterfield, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the **EASTERN** District of **OKLAHOMA** *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 21, United States Code, Section(s) 841 and 846, and the application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Charles Sutterfield, Task Force Officer
Task Force Officer with the DEA

Sworn to me.

Date: October 2, 2024

Judge's signature

City and state: Muskogee, Oklahoma

JASON A. ROBERTSON
UNITED STATES MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Charles Sutterfield, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property (digital devices) currently in law enforcement possession, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am an Agent with the Oklahoma Bureau of Narcotics (OBN) and have been since May 9, 2023. Prior to my career with OBN as an Agent, I was employed by the McAlester Police Department for approximately fifteen years as a full-time police officer. As an Agent I, investigate violations of the Uniform Controlled Dangerous Substances Act contained in Title 63 of the Oklahoma Statutes. I am a certified law enforcement officer by the Council on Law Enforcement Education and Training (CLEET) and was so certified in August 2006. I am a sworn Task Force Officer (TFO) with the Drug Enforcement Administration (DEA) and have been since January 2024.

3. I have attended training specific to the investigation of illegal drug offenses provided by the Oklahoma Bureau of Narcotics and the DEA. My experience includes, but is not limited to roadside investigations, interviews, and executing vehicle searches relating to numerous offenses including drug crimes. I have consulted with other experienced officers in narcotics investigations, and I have worked with other local, state, and federal law enforcement agencies.

4. I am familiar with the facts and circumstances of this investigation as a result of my personal participation in the investigation referred to in this affidavit and information summarized

in reports I have reviewed. I have compiled information derived from discussions with experienced law enforcement officers, including Special Agents of the DEA, and other state and local law enforcement agencies. Based on my training, experience and on my participation in this investigation, I know the following:

a. Fentanyl is a Schedule II controlled substance, and that the manufacture, distribution or possession with intent to distribute and conspiracy to commit said acts are violations of Title 21, United States Code, Sections 841(a)(1).

b. Drug traffickers commonly possess and/or use multiple cellular devices and/or methods of communication. Drug traffickers typically maintain a cellular device for daily communication with family/friends/associates, and frequently utilize a separate cellular device to facilitate the acquisition, transportation, and/or distribution of illegal controlled substances. Additionally, many drug traffickers regularly change telephone numbers and/or devices used to facilitate transactions in efforts to avoid law enforcement detection. Cellular telephones and other electronic devices that access the internet, are frequently used to send and receive messages over long distances through various applications.

c. Drug traffickers commonly use multiple cellular phones or other electronic devices to communicate with users and sellers of illegal controlled substances, negotiate prices for illegal controlled substances, solicit sales of illegal controlled substances, facilitate transactions where illegal controlled substances are sold, and photograph or video record money and drugs

obtained through illegal means. Use of a cellular telephone for such purposes is a violation of Title 21, United States Code, Section 843(b).

d. Drug traffickers, including couriers transporting drugs, use Global Positioning System (GPS) devices to assist them in navigation from locations where they start a trip to transport drugs to the intended destination where they deliver the drugs, which is often a great distance from where their trip started. Drug traffickers frequently maintain records, receipts, notes, ledgers, and other documents relating to the transportation, ordering, sale and distribution of controlled substances. Drug traffickers commonly consign controlled substances to their clients and transporters. The aforementioned records, receipts, notes, ledgers, and other documents are frequently stored on, maintained by or accessed using cellular telephones or other electronic devices where the traffickers have ready access to them.

e. Electronic files can be easily moved from one cellular phone or electronic storage medium to another. Therefore, electronic files downloaded to, or created on one cellular phone can be copied to, or transferred to, most any other cellular phone or storage medium.

f. Drug traffickers amass proceeds from the sale of drugs that the drug traffickers attempt to legitimize. Drug traffickers utilize domestic banks and their attendant services, securities, cashier checks, money drafts, letters of credit, brokerage houses, real estate, shell corporations, business fronts, and other forms of online virtual currency.

5. As a federal task force officer, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued

under the authority of the United States.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is described as a Cloud Mobile Stratus C7, IMEI: 356225738710543, ("Device 3"). Device 3 is currently in the possession of the Drug Enforcement Administration, McAlester Resident Office (MRO), at 100 Airport Road, McAlester, Oklahoma, located within the Eastern District of Oklahoma.

8. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. This affidavit is written in support of an ongoing investigation into the drug trafficking activities of Miranda Leann Clouse ("CLOUSE"). In August of 2024, the DEA MRO opened an investigation into the fentanyl trafficking activities of CLOUSE.

10. On August 9, 2024, DEA Task Force Officer (TFO) Chuck Sutterfield received information from an OBN confidential informant ("CI"), CSM-23-003, regarding CLOUSE who lives at 1020 E. Polk Ave, Apt #23 McAlester, Oklahoma 74501 ("CLOUSE Residence"), within the Eastern District of Oklahoma. The CI messaged TFO Sutterfield pictures of a rental vehicle CLOUSE was currently driving to Tulsa, Oklahoma to purchase fentanyl. Later the same day, TFO Sutterfield drove by CLOUSE's Residence and confirmed the license plate on the rental vehicle

the CI indicated CLOUSE was driving. TFO Sutterfield observed the license plate to be an Arizona tag: CWS-6515 on a silver Dodge Ram pickup. TFO Sutterfield entered the tag into a license plate reader system to monitor its movements.

11. On August 15, 2024, TFO Sutterfield was contacted by the CI at approximately 7:45 a.m., stating CLOUSE was about to travel to Tulsa, Oklahoma to purchase fentanyl. TFO Sutterfield drove by CLOUSE's Residence and noticed CLOUSE and another subject sitting in the truck. TFO Sutterfield contacted agents with the DEA MRO and initiated surveillance on CLOUSE's Residence. Agents maintained surveillance on CLOUSE as she traveled to multiple locations in McAlester, Oklahoma. One of the locations CLOUSE stopped at is a known residence where fentanyl was being distributed. After her drive, CLOUSE returned to her Residence where she remained for the rest of the day. The CI contacted CLOUSE and was told she was not going to Tulsa that day to purchase fentanyl. Agents with the MRO ended surveillance on CLOUSE at her Residence.

12. On August 17, 2024, TFO Sutterfield received multiple notifications from the license plate readers that the silver Dodge pickup with Arizona plate CWS-6515 was in the Tulsa, Oklahoma area. TFO Sutterfield had the CI contact CLOUSE to see if she was picking up fentanyl, and to see when she would return to McAlester. The CI informed TFO Sutterfield that CLOUSE was picking up fentanyl but was unsure when she would return to McAlester.

13. On August 20, 2024, TFO Sutterfield received a notification from the license plate readers that the silver Dodge Pickup with Arizona Plate CWS-6515 was in the Tulsa, Oklahoma

area near where it was located on August 17, 2024. TFO Sutterfield had the CI contact CLOUSE to see if she was in Tulsa to purchase fentanyl. The CI was told the rental truck that CLOUSE was driving had been impounded and CLOUSE was not in Tulsa. TFO Sutterfield along with other Agents with the MRO decided to set up surveillance in Okmulgee, Oklahoma to try and locate the silver Dodge pickup as it returned to McAlester. Agents with the MRO were able to locate the silver Dodge pickup traveling south on US-Highway 75 south of Okmulgee, Oklahoma. Agents with the MRO and the Oklahoma Highway Patrol were able to coordinate a traffic stop of the vehicle on US-Highway 75 approximately four miles south of Okmulgee, Oklahoma. CLOUSE and a male driver who was identified as Tylor CASEY were found to be in possession of a powdery substance later determined to be fentanyl powder, and methamphetamine. CLOUSE and CASEY were subsequently arrested and booked into the Okmulgee County Jail for Trafficking fentanyl and Possession of Drug Paraphernalia.

14. During post arrest interviews with CLOUSE AND CASEY, they both signed Miranda waivers and Consent to Search forms for their cellular devices. CASEY identified the iPhone with black case, bearing IMEI: 356866114437209 ("Device 1") as belonging to him. During the interview, both CLOUSE and CASEY admitted to traveling to Tulsa previously to purchase fentanyl powder for personal use and distribution in McAlester, Oklahoma. CLOUSE and CASEY admitted that on August 20, 2024, they traveled to Tulsa, Oklahoma to purchase powder fentanyl. TFO Kevin Fox photographed images of a Taurus handgun with serial number 1KA22569 that CASEY had a picture of saved on Device 1. CLOUSE admitted she dropped

CASEY off at his friend's house to trade a gun and tools for fentanyl. CLOUSE stated she went to Tulsa to purchase powder fentanyl from her source of supply. CLOUSE stated she called her source of supply from her Samsung cell phone ("Device 2"), IMEI:353122993256119, and was advised to meet with a driver at a Family Dollar store on 33rd Street in Tulsa, Oklahoma. CLOUSE admitted to purchasing two grams of powder fentanyl from her source of supply. CLOUSE admitted her fentanyl source of supply that she purchased fentanyl from earlier that evening was saved in Device 2 as "An And Be Back." During the interview, CASEY said he texted a female named "Goldie" from Device 1 to set up the trade of a gun and tools for powder fentanyl. CASEY admitted he traded a gun and tools for approximately five or six grams of powder fentanyl that evening. TFO Fox photographed a Facebook Messenger conversation between CASEY and Goldi Renee. In the Facebook Messenger conversation, CASEY states he is on his way to Tulsa and is asking for an address to meet with Goldi. CLOUSE later admitted that she uses a Cloud Mobil cell phone as a Wi-Fi only phone to communicate with Paul Parker a/k/a "PJ" to set up drug transactions ("Device 3"), IMEI: 356225738710543. CLOUSE stated that Paul Parker is one of her main purchasers of fentanyl who lived in McAlester, Oklahoma. Device 3 was not viewed during the interview because Device 3's battery was dead.

15. Additionally, CLOUSE admitted to purchasing fentanyl from an unknown Hispanic male, ("UM"), in the Tulsa, Oklahoma area for approximately the last four months. CLOUSE admitted she had been purchasing 1-ounce quantities of fentanyl from UM for $1,100.00 per ounce, and in the past four months she had purchased 1 ounce of fentanyl on ten different

occasions. CLOUSE stated, over the past four months, she also purchased smaller quantity amounts of fentanyl for $50.00 a gram. CLOUSE stated she has bought powder fentanyl from UM less than 20 times over the past four months. CLOUSE stated UM's contact was saved on Device 2 as "An And Be Back", and also "The Mexican".

16. Additionally, CASEY admitted to living with CLOUSE and her boyfriend Heath Carter in McAlester, Oklahoma for the last two months. During the interview with CASEY, your affiant viewed text message communications discussing the purchase of drugs between CASEY and Heath Carter on Device 1.

17. Device 3 is currently in the lawful possession of the possession of the DEA, MRO, at 100 Airport Road, McAlester, Oklahoma. It came into the DEA's possession after Device 3 was seized incident to arrest. Additionally, CLOUSE provided consent to search Device 3. Therefore, while the DEA might already have all necessary authority to examine Device 3, I seek this additional warrant out of an abundance of caution to be certain that an examination of Device 3 will comply with the Fourth Amendment and other applicable laws.

18. The Device is currently in storage at 100 Airport Road, McAlester, Oklahoma. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

b. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (e.g.,

149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many

ISPs assign each subscriber an account name, a username or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

e. "Peer to Peer file sharing" ("P2P") is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

(1) When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by

copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

(2) Third party software is available to identify the IP address of a P2Pcomputer that is sending a file. Such software monitors and logs Internet and local network traffic.

20. Based on my training, experience, and research, I know that the cellular telephone described in Attachment A has capabilities that allow it to serve as a wireless telephone, digital camera, GPS navigation device, and to browse the internet. In my training and experience, examining data stored on this type of device can uncover evidence described in Attachment B, and among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication, who did not, as well as evidence relating to the commission of the offense under investigation.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application Seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how Device 3 was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on Device 3 because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators.

Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of Device 3 consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

26. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a

particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and

extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected

time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

g. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

(1) The digital devices, and/or any digital images thereof created by law enforcement in aid of the examination and review, will be examined and reviewed by law enforcement personnel, sometimes with the aid of a technical expert, in an appropriate setting, in order to extract and seize the information, records, or evidence described in Attachment B.

(2) The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic

storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

(3) In searching the digital devices, the forensic examiners may examine as much of the contents of the devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

CONCLUSION

27. I respectfully submit that this affidavit supports probable cause for a warrant to the Device described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

Chuck Sutterfield, Task Force Officer
Drug Enforcement Administration

Sworn on October 2. 2024:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched.

1. The property to be searched is described as a Cloud Mobile Stratus C7 IMEI: 356225738710543, ("Device 3"). Device 3 is currently in the possession of the Drug Enforcement Administration, McAlester Resident Office (MRO), at 100 Airport Road, McAlester, Oklahoma, located within the Eastern District of Oklahoma.

ATTACHMENT B

Property to be seized

1. All records on the Device described in Attachment A that relate to violations of 21 U.S.C. 841(a)(1) and 846, Possession with the Intent to Distribute Fentanyl which involve Miranda CLOUSE and others as yet identified, including:

a. lists of customers/associates and related identifying information;

b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

d. any information recording CLOUSE's, or other co-conspirators schedule or recent travel;

e. all bank records, checks, credit card bills, account information, and other financial records.

f. communications including text messages or recorded voice messages saved on the Device, as well as call history, stored telephone numbers and other notes ;

g. photographs or videos which may identify, drugs, drug proceeds, items obtained with drug proceeds, co-conspirators or locations;

h. stored addresses or locations within mapping software that may identify locations recently visited.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.